WHAT IS CLAIMED IS:

1. A method for preventing unauthorized use of software accessing at least one specific hardware module comprising a unique hardware identification sequence wherein said software comprises a license key for being executed, comprising:

   - reading out said hardware identification sequence of said at least one specific hardware module,

   - retrieving a predetermined hardware identification sequence contained in said license key,

   - comparing said read-out hardware identification sequence with said hardware identification sequence contained in the license key; and

   - permitting execution of said software if both sequences match.

2. The method according to claim 1, wherein said hardware identification sequence contained in said license key is encrypted.

3. The method according to claim 2, wherein a secret key coded in said software is used to decrypt said hardware identification sequence.

4. The method according to claim 2, wherein a secret algorithm coded in said software is used to decrypt said hardware identification sequences.

5. The method according to claim 2, wherein a public key encryption method is used for encrypting and decrypting said unique hardware identification sequence contained in said license key, comprising:

- a secret key which is only known to the license key distribution authorities and

- a public key corresponding to said secret key,

wherein said secret key is used for encrypting said hardware identification sequence and said public key is used for decrypting said hardware identification sequence and wherein said public key is the only key which allows to decrypt data encrypted by the secret key.

6. The method according to claim 5, wherein said public key is encrypted additionally using a public key encryption method, comprising:

- a second secret key which is only known to a trusted third authority and

- a second public key corresponding to said second secret key,

wherein said second secret key is used for encrypting said public key and said second public key is used for decrypting said encrypted public key and wherein said second public key is the only key which allows to decrypt data encrypted by the second secret key.

7. The method according to claim 1, wherein at least one of the public key is accessible freely.

5 8. The method according to anyone of the preceding claims, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address (MAC).

10 9. The method according to claim 8, wherein at least one of said specific hardware modules is a Bluetooth™ module comprising a unique Bluetooth™ hardware address.

10. The method according to claim 2, wherein at least one
15 of the public key is accessible freely.

11. The method according to claim 3, wherein at least one of the public key is accessible freely.

20 12. The method according to claim 4, wherein at least one of the public keys is accessible freely.

13. The method according to claim 5, wherein at least one of the public key is accessible freely.

25

14. The method according to claim 6, wherein at least one of the public key is accessible freely.

15. The method according to claim 2, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address (MAC).

16. The method according to claim 3, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address (MAC).

17. The method according to claim 4, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address (MAC).

18. The method according to claim 5, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address (MAC).

19. The method according to claim 6, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address (MAC).

20. The method according to claim 7, wherein at least one of said specific hardware modules is a network interface module comprising a unique network interface address (MAC).

5